Certificatore Accreditato Poste Italiane S.p.A.

Servizio Postecert Firma Digitale

Guida alla comprensione degli OID presenti nei certificati rilasciati da Poste Italiane S.p.A.

Indice

1 Introduzione

Poste Italiane, in quanto Prestatore di Servizi Fiduciari Qualificati, a partire dal 01/04/2017 emette certificati digitale delle seguenti tipologie:

- Certificati relativi ad Autorità di Certificazione
- Certificati Qualificati per la Firma Elettronica Qualificata e Firma Digitale
- Certificati Elettronici
- Certificati di Marcatura Temporale
- Certificati per Carta Nazionale dei Servizi

Il 30 Gennaio 2017 è intervenuta la fusione per incorporazione, con efficacia dal 1° Aprile 2017, di Postecom S.p.A in Poste Italiane S.p.A. A partire da tale data (1° aprile 2017), Poste Italiane subentra, conseguentemente, in tutti i rapporti (attivi e passivi), nei diritti e negli obblighi facenti capo a Postecom. In particolare Poste italiane prende in carico la gestione del ciclo di vita dei certificati emessi da Postecom fino al 31/03/2017 come Certificatore Accreditato, che appartengono alle seguenti tipologie:

- Certificati relativi ad Autorità di Certificazione
- Certificati Qualificati per la Firma Elettronica Qualificata e Firma Digitale
- Certificati Elettronici
- Certificati per Web Server e firma codice
- Certificati di Marcatura Temporale
- Certificati per Carta Nazionale dei Servizi

Ciascuna tipologia di certificato è individuata da uno o più OID (*Object Identifier*) che ne definiscono l'ambito di utilizzo. All'interno della struttura del certificato, il campo "Certificate Policy" contiene i relativi valori di OID.

2 Prestatore di Servizi Fiduciari Qualificati Poste Italiane

2.1 Certificati delle Autorità di certificazione

POSTE ITALIANE EU QUALIFIED CERTIFICATES CA (OID 1.3.76.48.1.4.1.1)

TIPOLOGIA	OID	DESCRIZIONE
Certificato Qualificato	1.3.76.48.1.2.3.4	CQ rilasciati a persone legali
	1.3.76.48.1.2.3.1	CQ rilasciati a persone fisiche, su dispositivo HSM, per firme remote
	1.3.76.48.1.2.3.2	CQ rilasciati a persone fisiche, su dispositivo HSM, per firme automatiche e/o firme verificate
	1.3.76.48.1.2.3.3	CQ rilasciati a persone fisiche, su dispositivo Smart Card

POSTE ITALIANE TIME STAMPING AUTHORITY (OID 2.5.29.32.0)

TIPOLOGIA	OID	DESCRIZIONE
Certificato di Marcatura Temporale	0.4.0.2023.1.1	Servizio di marcatura temporale

POSTE ITALIANE CA (OID 1.3.76.48.1.5.1.1)

TIPOLOGIA	OID	DESCRIZIONE
Certificato Elettronico Ausiliario	1.3.76.48.1.5.1.1.4	Certificato ausiliario
Certificato Elettronico	1.3.76.48.1.5.1.1.3	Dispositivo sw
	1.3.76.48.1.5.1.1.2	Dispositivo hw
Certificato Elettronico su supporto hw mobile	1.3.76.48.1.5.1.1.5	Certificato su supporto hw mobile

AUTORITÀ CHE RILASCIANO CERTIFICATI DI AUTENTICAZIONE PER CNS

TIPOLOGIA	OID	DESCRIZIONE
Certificato per CNS	1.3.76.16.2.1 1.3.76.48.1.3.1	Certificato di autenticazione per CNS

Tipologia di certificati emessi	Autorità di certificazione	PI EU QC CA	PI TSA	PI CA	CNS
		1.3.76.48.1.4.1.1	2.5.29.32.0	1.3.76.48.1.5.1.1	1.3.76.48.1.3.1
Certificati Qualificati persona legale	1.3.76.48.1.2.3.4	X			
Certificati Qualificati persona fisica –dispositivo HSM per firma remota	1.3.76.48.1.2.3.1	X			
Certificati Qualificati persona fisica –dispositivo HSM per firma automatica e/o verificata	1.3.76.48.1.2.3.2	X			
Certificati Qualificati persona fisica –dispositivo Smart Card	1.3.76.48.1.2.3.3	X			
Certificato di marca temporale (EU)	0.4.0.2023.1.1		X		
Certificati Elettronici - Ausiliari	1.3.76.48.1.5.1.1.2			X	
Certificati Elettronici - supporto sw	1.3.76.48.1.5.1.1.3			X	
Certificati Elettronici - supporto hw	1.3.76.48.1.5.1.1.4			X	
Certificati Elettronici - supporto hw mobile	1.3.76.48.1.5.1.1.5			X	
Certificato di autenticazione per CNS	1.3.76.16.2.1				X

2.2 Certificati qualificati

OID	DESCRIZIONE
1.3.76.48.1.2.3.4	Certificato Qualificato rilasciato a persone legali
1.3.76.48.1.2.3.1	Certificato Qualificato rilasciato a persone fisiche, su dispositivo HSM, per firme remote
1.3.76.48.1.2.3.2	Certificato Qualificato rilasciato a persone fisiche, su dispositivo HSM, per firme automatiche e/o firme verificate
1.3.76.48.1.2.3.3	Certificato Qualificato rilasciato a persone fisiche, su dispositivo Smart Card

I certificati qualificati sono rilasciati dall'Autorità di certificazione:

- **Poste Italiane EU Qualified Certificates CA (OID 1.3.76.48.1.4.1.1)**

Poste Italiane, in qualità di Prestatore di Servizi Fiduciari Qualificati ai sensi del **Regolamento UE n.910/2014 (eIDAS)**, rilascia certificati qualificati secondo quanto descritto all'interno del "Manuale Operativo", del "Certification Practice Statement and Certificate Policy" e del "PKI Disclosure Statement" depositati presso l'Agenzia per l'Italia Digitale e disponibili on-line sul sito Postecert (http://postecert.poste.it/index.shtml sezione firma digitale).

2.2.1 Certificato Qualificato rilasciato a persone legali

Il profilo dei certificati qualificati emessi prevede la valorizzazione dei campi così come stabilito dal citato Regolamento UE n.910/2014 (eIDAS).

Nome del campo	Descrizione
givenName (2.5.4.42) Surname (2.5.4.4)	Contengono rispettivamente il nome ed il cognome del rappresentante legale della persona legale
OrganizationName (2.5.4.10) Organization identifier (2.5.4.97)	Se applicabili, contengono le informazioni relative alla persona legale a cui è rilasciato il certificato
Dn_Qualifier (2.5.4.46)	Contiene il codice identificativo univoco del titolare presso il certificatore
QcStatements	
1- QcCompliance (0.4.0.1862.1.1)	Indica che il certificato è qualificato
2- QcEuLimitValue (0.4.0.1862.1.2)	Contiene, se applicabile, il limite di negoziazione
3- QcEuRetentionPeriod	Indica il tempo di conservazione della documentazione da parte del

(0.4.0.1862.1.3)	certificatore, pari a 20 anni
4- QcSSCD (0.4.0.1862.1.4)	Indica che la chiave crittografica risiede su un dispositivo sicuro
5- QcEuPDS (0.4.0.1862.1.5)	Contiene la url dove reperire il "PKI Disclosure Statements"
KeyUsage (2.5.29.15)	Contiene il valore "non repudiation" ad indicare la firma apposta con tale certificato ha il valore legale
CertificatePolicies	Contiene l'OID relativo alla tipologia del certificato (1.3.76.48.1.2.3.4). Contiene, se applicabile, una limitazione d'uso del certificato.

2.2.2 Certificato Qualificato rilasciato a persone fisiche

Il profilo dei certificati qualificati emessi prevede la valorizzazione dei campi così come stabilito dal citato Regolamento UE n.910/2014 (eIDAS).

Nome del campo	**Descrizione**
givenName (2.5.4.42) Surname (2.5.4.4)	Contengono rispettivamente il nome ed il cognome del titolare del certificato
SerialNumber (2.5.4.5)	Contiene il numero del documento di riconoscimento del titolare del certificato, preceduto da una codice che identifica la tipologia di documento.
OrganizationName (2.5.4.10) Organization identifier (2.5.4.97)	Se applicabili, contengono le informazioni relative all'organizzazione di appartenenza del titolare del certificato, che ha autorizzato il rilascio del certificato stesso.
Dn_Qualifier (2.5.4.46)	Contiene il codice identificativo univoco del titolare presso il certificatore
QcStatements	
1- QcCompliance (0.4.0.1862.1.1)	Indica che il certificato è qualificato
2- QcEuLimitValue (0.4.0.1862.1.2)	Contiene, se applicabile, il limite di negoziazione
3- QcEuRetentionPeriod (0.4.0.1862.1.3)	Indica il tempo di conservazione della documentazione, pari a 20 anni
4- QcSSCD (0.4.0.1862.1.4)	Indica che la chiave crittografica risiede su un dispositivo sicuro
5- QcEuPDS (0.4.0.1862.1.5)	Contiene la url dove reperire il "PKI Disclosure Statements"
KeyUsage (2.5.29.15)	Contiene il valore "non repudiation" ad indicare la firma apposta con tale certificato ha il valore legale

CertificatePolicies	Contiene l'OID relativo alla tipologia del certificato (1.3.76.48.1.2.3.1 o 1.3.76.48.1.2.3.2 o 1.3.76.48.1.2.3.3). Contiene, se applicabile, una limitazione d'uso del certificato.

2.3 Certificati di marcatura temporale

OID	DESCRIZIONE
0.4.0.2023.1.1	Certificato di marca temporale

I certificati qualificati sono stati rilasciati dall'Autorità di certificazione:

- **Poste Italiane Time Stamping Authority (OID 2.5.29.32.0)**

I certificati di marcatura temporale vengono utilizzati per sottoscrivere marche temporali associate a documenti elettronici. Le marche temporali permettono di associare data e ora certe e opponibili a terzi ai documenti ai quali sono apposte.

Poste Italiane, in qualità di Prestatore di Servizi Fiduciari Qualificati ai sensi del **Regolamento UE n.910/2014 (eIDAS)**, rilascia certificati qualificati secondo quanto descritto all'interno del "Manuale Operativo", del "Certification Practice Statement and Certificate Policy" e del "PKI Disclosure Statement" depositati presso l'Agenzia per l'Italia Digitale e disponibili on-line sul sito Postecert (http://postecert.poste.it/index.shtml sezione marche temporali).

Il profilo dei certificati qualificati emessi prevede la valorizzazione dei campi così come stabilito dal citato Regolamento UE n.910/2014 (eIDAS).

2.4 Certificati Elettronici

2.4.1 Certificati elettronici Ausiliari

OID	DESCRIZIONE
1.3.76.48.1.5.1.1.2	Certificato Elettronici Ausiliari

I certificati elettronici ausiliari sono rilasciati dall'Autorità di certificazione:

- **Poste Italiane CA (OID 1.3.76.48.1.5.1.1)**

I Certificati Elettronici Ausiliari sono certificati elettronici emessi su smart card (unitamente o meno ai certificati qualificati a seconda del tipo di fornitura) che consentono all'utente di: autenticarsi a siti e portali in modalità https (*strong authentication*), cifrare documenti elettronici tramite l'applicativo di firma distribuito dal

certificatore, utilizzare le funzionalità crittografiche messe a disposizione in ambiente Microsoft (ad es. firma e cifratura di e-mail), apporre una firma elettronica.

Il profilo dei certificati elettronici ausiliari prevede quanto segue.

Nome del campo	Descrizione
givenName (2.5.4.42) Surname (2.5.4.4)	Contengono rispettivamente il nome ed il cognome del titolare del certificato
OrganizationName (2.5.4.10)	Se applicabile, contiene le informazioni relative all'organizzazione di appartenenza del titolare del certificato, che ha autorizzato il rilascio del certificato stesso.
KeyUsage (2.5.29.15)	Contiene il valore "Digital signature,Key encipherment,Data encipherment"
CertificatePolicies	Contiene l'OID relativo alla tipologia del certificato (1.3.76.48.1.5.1.1.2)

2.4.2 Certificati elettronici su supporto hw e sw e su supporto hw mobile

OID	Descrizione
1.3.76.48.1.5.1.1.2	Supporto hardware
1.3.76.48.1.5.1.1.3	Supporto software
1.3.76.48.1.5.1.1.5	Supporto hw mobile

I certificati elettronici ausiliari sono rilasciati dall'Autorità di certificazione:

- **Poste Italiane CA (OID 1.3.76.48.1.5.1.1)**

I certificati elettronici possono essere utilizzati nell'ambito di funzionalità crittografiche legate alla cifratura, l'autenticazione, la firma elettronica. A differenza dei certificati elettronici ausiliari, non sono necessariamente emessi su dispositivo sicuro e contestualmente al rilascio di un certificato qualificato. Il processo di erogazione pertanto impone meno vincoli rispetto al processo di erogazione dei certificati ausiliari, ad esempio non è prevista l'identificazione certa del titolare.

I certificati su supporto hw mobile si riferiscono a chiavi crittografiche presenti a bordo di carte SIM per servizi di telefonia mobile, utilizzate nell'ambito di servizi aggiunti offerti dall'operatore mobile

2.5 Certificati per CNS

OID	Tipologia di certificati
1.3.76.16.2.1 1.3.76.48.1.3.1	Certificato di autenticazione per CNS

Poste Italiane emette certificati di autenticazione per carte CNS per conto di Province e Regioni Autonome, tramite Autorità di certificazione appositamente dedicate, nell'ambito della fornitura, da parte di Sogei verso i cittadini, di carte CNS con funzioni di Tessera Sanitaria.

3 Certificatore Accreditato Postecom

3.1 Certificati delle Autorità di certificazione

POSTECOM CA1 (OID 1.3.76.11.1.2.1.1)

Certificati emessi fino al 30/06/2016

TIPOLOGIA	OID	DESCRIZIONE
Certificato Qualificato	1.3.76.11.1.2.3.1	CQ
	1.3.76.11.1.2.3.2	CQ per firme automatiche
Certificato Elettronico Ausiliario	1.3.76.11.1.1.10.3	Certificato ausiliario
Certificato Elettronico	1.3.76.11.1.1.10.1	Dispositivo hw
	1.3.76.11.1.1.10.2	Dispositivo sw
Certificato supporto hw mobile	1.3.76.11.1.1.10.4	Certificato supporto hw mobile

POSTECOM CA2 (OID 2.5.29.32.0)

Scaduta il 10/05/2016

TIPOLOGIA	OID	DESCRIZIONE
Certificato Qualificato	1.3.76.11.1.2.3.1	CQ
	1.3.76.11.1.2.3.2	CQ per firme automatiche
Certificato Elettronico Ausiliario	1.3.76.11.1.1.10.3	Certificato ausiliario
Certificato Elettronico	1.3.76.11.1.1.10.1 oppure 1.3.76.11.11.5.1	Dispositivo hw
	1.3.76.11.1.1.10.2	Dispositivo sw
Certificato supporto hw mobile	1.3.76.11.1.1.10.4	Certificato supporto hw mobile
Certificato per CNS	1.3.76.11.1.3.1	Certificato di autenticazione per CNS

POSTECOM CA3 (OID 2.5.29.32.0)

Certificati emessi fino al 30/06/2016

TIPOLOGIA	OID	DESCRIZIONE
Certificato Qualificato	1.3.76.11.1.2.3.1	CQ
	1.3.76.11.1.2.3.2	CQ per firme automatiche
Certificato Elettronico Ausiliario	1.3.76.11.1.1.10.3	Certificato ausiliario
Certificato Elettronico	1.3.76.11.1.1.10.1 oppure 1.3.76.11.11.5.1	Dispositivo hw
	1.3.76.11.1.1.10.2	Dispositivo sw
Certificato supporto hw mobile	1.3.76.11.1.1.10.4	Certificato supporto hw mobile
Certificato per CNS	1.3.76.11.1.3.1	Certificato di autenticazione per CNS

Certificati emessi a partire dal 01/07/2016 fino al 31/03/2017

TIPOLOGIA	OID	DESCRIZIONE
Certificato Qualificato	1.3.76.11.1.2.3.1	CQ
	1.3.76.11.1.2.3.2	CQ per firme automatiche

POSTECOM CA4 (OID 1.3.76.11.1.1.6.1)

Certificati emessi a partire dal 01/07/2016 fino al 31/03/2017

TIPOLOGIA	OID	DESCRIZIONE
Certificato elettronico	1.3.76.11.1.1.10.1	Dispositivo hw
	1.3.76.11.1.1.10.2	Dispositivo sw
	1.3.76.11.1.1.10.3	Certificato ausiliario
	1.3.76.11.1.1.10.10	Certificati Elettronici IDABC
	1.3.76.11.1.1.4.2	Certificati SSL client
	1.3.76.11.1.1.4.3	Certificati firma codice

POSTECOM CA5 (OID 1.3.76.11.1.1.6.1)

Certificati emessi fino al 31/03/2017

TIPOLOGIA	OID	DESCRIZIONE
Certificato Elettronico	1.3.76.11.1.1.10.4	Certificato supporto hw mobile

POSTECOM CS1 (OID 1.3.76.11.1.1.6.1)

Certificati emessi fino al 31/03/2017

TIPOLOGIA	OID	DESCRIZIONE
Certificato elettronico	1.3.76.11.1.1.10.1	Dispositivo hw
	1.3.76.11.1.1.10.2	Dispositivo sw
	1.3.76.11.1.1.10.10	Certificati Elettronici IDABC
	1.3.76.11.1.1.6.2	Certificati di sicurezza (Firma codice)

POSTECOM CS2, POSTECOM CS3 (OID 1.3.76.11.1.1.3.1)

Certificati emessi fino al 31/03/2017

TIPOLOGIA	OID	DESCRIZIONE
Certificato per web server	1.3.76.11.1.1.4.1	Certificati SSL Web Server
	1.3.76.11.1.1.4.2	Certificati SSL Client
	1.3.76.11.1.1.4.3	Certificati Firma codice

POSTECOM TIME STAMPER CA2 (OID 1.3.76.11.1.2.1.1)

Certificati emessi fino al 31/03/2017

TIPOLOGIA	OID	DESCRIZIONE
Certificato di Marcatura Temporale	1.3.76.11.1.2.2.1	Servizio di marcatura temporale

AUTORITÀ CHE RILASCIANO CERTIFICATI DI AUTENTICAZIONE PER CNS (OID 1.3.76.11.1.3.1)

TIPOLOGIA	OID	DESCRIZIONE
Certificato per CNS	1.3.76.16.2.1	Certificato di autenticazione per CNS

Schema valido fino al 30/06/2016

Tipologia di certificati emessi	Autorità di certificazione	CA1	CA2	CA3	CA4	CA5	CS1	CS2	CS3	TS CA2	CNS
		1.3.76.11.1.2.1.1	2.5.29.32.0		1.3.76.11.1.1.6.1			1.3.76.11.1.1.3.1		1.3.76.11.1.2.1.1	1.3.76.11.1.3.1
Certificati qualificati	1.3.76.11.1.2.3.1	X	X	X							
Certificati qualificati - Firma automatica	1.3.76.11.1.2.3.2	X	X	X							
Certificato di marca temporale	1.3.76.11.1.2.2.1									X	
Certificati Elettronici - Ausiliari	1.3.76.11.1.1.10.3	X	X	X	X						
Certificati Elettronici - supporto hw	1.3.76.11.1.1.10.1	X	X	X	X		X				
Certificati Elettronici - supporto sw	1.3.76.11.1.1.10.2	X	X	X	X		X				
Supporto hw	1.3.76.11.11.5.1		X	X							
Certificati Elettronici IDABC	1.3.76.11.1.1.10.10				X		X				
Certificati Elettronici - supporto hw mobile	1.3.76.11.1.1.10.4	X	X	X		X					
Certificati di sicurezza (Firma codice)	1.3.76.11.1.1.6.2						X				
Certificati SSL Web Server	1.3.76.11.1.1.4.1							X	X		
Certificati SSL Client	1.3.76.11.1.1.4.2				X			X	X		
Certificati Firma codice	1.3.76.11.1.1.4.3				X			X	X		
Certificato di autenticazione CNS	1.3.76.16.2.1										X

Schema valido dal 01/07/2016 al 31/03/2017

Tipologia di certificati emessi	**Autorità di certificazione**	**CA3**	**CA4**	**CA5**	**CS1**	**CNS**	**CS3**	**TS CA2**	**CNS**
		2.5.29.32.0	1.3.76.11.1.1.6.1			1.3.76.11.1.1.3.1		1.3.76.11 .1.2.1.1	1.3.76.11 .1.3.1
Certificati qualificati	1.3.76.11.1.2.3.1	X							
Certificati qualificati - Firma automatica	1.3.76.11.1.2.3.2	X							
Certificato di marca temporale	1.3.76.11.1.2.2.1							X	
Certificati Elettronici - Ausiliari	1.3.76.11.1.1.10.3		X						
Certificati Elettronici - supporto hw	1.3.76.11.1.1.10.1		X		X				
Certificati Elettronici - supporto sw	1.3.76.11.1.1.10.2		X		X				
Certificati Elettronici IDABC	1.3.76.11.1.1.10.10		X		X				
Certificati Elettronici - supporto hw mobile	1.3.76.11.1.1.10.4			X					
Certificati di sicurezza (Firma codice)	1.3.76.11.1.1.6.2				X				
Certificati SSL Web Server	1.3.76.11.1.1.4.1					X	X		
Certificati SSL Client	1.3.76.11.1.1.4.2		X			X	X		
Certificati Firma codice	1.3.76.11.1.1.4.3		X			X	X		
Certificato di autenticazione CNS	1.3.76.16.2.1								X

NOTA: variazioni rispetto alla tabella precedente:

- non sono presenti Postecom CA1 e Postecom CA2 (che non emettono certificati nel periodo considerato),
- Postecom CA3 emette solo certificati qualificati.

3.2 Certificati qualificati

OID	DESCRIZIONE
1.3.76.11.1.2.3.1	Certificato Qualificato
1.3.76.11.1.2.3.2	Certificato Qualificato utilizzato per l'apposizione di firme automatiche

I certificati qualificati sono stati rilasciati dalle seguenti Autorità di certificazione:

- **Postecom CA1 (OID 1.3.76.11.1.2.1.1),**
- **Postecom CA2 (OID 2.5.29.32.0),**
- **Postecom CA3 (OID 2.5.29.32.0).**

Postecom, in qualità di Certificatore Accreditato ai sensi della normativa italiana vigente, ha rilasciato fino al 31/03/2016 certificati qualificati secondo quanto descritto all'interno del "Manuale Operativo – Certificatore Accreditato Postecom S.p.A. – Servizio Postecert Firma Digitale" depositato presso l'Agenzia per l'Italia Digitale e disponibile on-line (http://postecert.poste.it/index.shtml sezione firma digitale).

Il profilo dei certificati qualificati emessi prevede la valorizzazione dei campi così come stabilito dalla Deliberazione CNIPA n.45 del 21 maggio 2009 (e s.m.i.).

Nome del campo	Descrizione
givenName (2.5.4.42) Surname (2.5.4.4)	Contengono rispettivamente il nome ed il cognome del titolare del certificato
SerialNumber (2.5.4.5)	Contiene il numero del codice fiscale del titolare del certificato
OrganizationName (2.5.4.10)	Se applicabile, contiene le informazioni relative all'organizzazione di appartenenza del titolare del certificato, che ha autorizzato il rilascio del certificato stesso.
Dn_Qualifier (2.5.4.46)	Contiene il codice identificativo univoco del titolare presso il certificatore
QcStatements	
1- QcCompliance (0.4.0.1862.1.1)	Indica che il certificato è qualificato
2- QcEuLimitValue (0.4.0.1862.1.2)	Contiene, se applicabile, il limite di negoziazione
3- QcEuRetentionPeriod (0.4.0.1862.1.3)	Indica il tempo di conservazione della documentazione, pari a 20 anni
4- QcSSCD (0.4.0.1862.1.4)	Indica che la chiave crittografica risiede su un dispositivo sicuro
KeyUsage (2.5.29.15)	Contiene il valore "non repudiation" ad indicare la firma apposta con tale certificato ha il valore legale

CertificatePolicies	Contiene l'OID relativo alla tipologia del certificato (1.3.76.11.1.2.3.1 o 1.3.76.11.1.2.3.2). Contiene, se applicabile, una limitazione d'uso del certificato ad un particolare contesto.

3.3 Certificati di marcatura temporale

OID	DESCRIZIONE
1.3.76.11.1.2.2.1	Certificato di marca temporale

I certificati di marca temporale sono stati rilasciati dall'Autorità di certificazione:

- **Postecom Time Stamper CA2 (OID 1.3.76.11.1.2.1.1)**

I certificati di marcatura temporale vengono utilizzati per sottoscrivere marche temporali associate a documenti elettronici. Le marche temporali permettono di associare data e ora certe e opponibili a terzi ai documenti ai quali sono apposte.

Postecom, in qualità di Certificatore Accreditato ai sensi della normativa italiana vigente, ha rilasciato fino al 31/03/2016 certificati di marcatura temporale secondo quanto descritto all'interno del "Manuale Operativo – Certificatore Accreditato Postecom S.p.A. – Servizio Postecert Firma Digitale" depositato presso l'Agenzia per l'Italia Digitale e disponibile on-line (http://postecert.poste.it/index.shtml sezione firma digitale).

Il profilo dei certificati qualificati emessi prevede la valorizzazione dei campi così come stabilito dalla Deliberazione CNIPA n.45 del 21 maggio 2009 (e s.m.i.).

3.4 Certificati Elettronici

3.4.1 Certificati Elettronici Ausiliari

OID	DESCRIZIONE
1.3.76.11.1.1.10.3	Certificato Elettronici Ausiliari

I certificati elettronici ausiliari sono stati rilasciati dalle seguenti Autorità di certificazione:

- fino al 30/06/2016:
  - **Postecom CA1 (OID 1.3.76.11.1.2.1.1)**,
  - **Postecom CA2 (OID 2.5.29.32.0)**,
  - **Postecom CA3 (OID 2.5.29.32.0)**,
- a partire dal 01/07/2016 fino al 31/03/2017:

- **Postecom CA4 (OID 1.3.76.11.1.1.6.1).**

I Certificati Elettronici Ausiliari sono certificati elettronici emessi su smart card (unitamente o meno ai certificati qualificati a seconda del tipo di fornitura) che consentono all'utente di: autenticarsi a siti e portali in modalità https (*strong authentication*), cifrare documenti elettronici tramite l'applicativo di firma distribuito dal certificatore, utilizzare le funzionalità crittografiche messe a disposizione in ambiente Microsoft (ad es. firma e cifratura di e-mail), apporre una firma elettronica.

Il profilo dei certificati elettronici ausiliari prevede quanto segue.

Nome del campo	Descrizione
givenName (2.5.4.42) Surname (2.5.4.4)	Contengono rispettivamente il nome ed il cognome del titolare del certificato
OrganizationName (2.5.4.10)	Se applicabile, contiene le informazioni relative all'organizzazione di appartenenza del titolare del certificato, che ha autorizzato il rilascio del certificato stesso.
KeyUsage (2.5.29.15)	Contiene il valore "Digital signature,Key encipherment,Data encipherment"
CertificatePolicies	Contiene l'OID relativo alla tipologia del certificato (1.3.76.11.1.1.10.3)

3.4.2 Certificati Elettronici su supporto hw e sw

OID	Descrizione
1.3.76.11.1.1.10.1 oppure 1.3.76.11.1.1.5.1	Supporto hardware
1.3.76.11.1.1.10.2	Supporto software
1.3.76.11.1.1.10.10	Certificati Elettronici IDABC

I certificati elettronici su supporti hw e sw sono stati rilasciati dalle seguenti Autorità di certificazione:

- fino al 30/06/2016 :
  - **Postecom CA1 (OID 1.3.76.11.1.2.1.1)**,
  - **Postecom CA2 (OID 2.5.29.32.0),**
  - **Postecom CA3 (OID 2.5.29.32.0)**,
  - **Postecom CS1 (OID 1.3.76.11.1.1.6.1)**,
- a partire dal 01/07/2016 fino al 31/03/2017:
  - **Postecom CS1 (OID 1.3.76.11.1.1.6.1)**,
  - **Postecom CA4 (OID 1.3.76.11.1.1.6.1)**.

I certificati elettronici possono essere utilizzati nell'ambito di funzionalità crittografiche legate alla cifratura, l'autenticazione, la firma elettronica. A differenza dei certificati elettronici ausiliari, non sono necessariamente emessi su dispositivo sicuro e contestualmente al rilascio di un certificato qualificato. Il processo di erogazione pertanto impone meno vincoli rispetto al processo di erogazione dei certificati ausiliari, ad esempio non è prevista l'identificazione certa del titolare.

3.4.3 Certificati Elettronici su supporto hw mobile

OID	Descrizione
1.3.76.11.1.1.10.4	Supporto hardware mobile

I certificati elettronici su supporto hw mobile sono stati rilasciati dalle seguenti Autorità di certificazione:

- fino al 30/06/2016 :
  - **Postecom CA1 (OID 1.3.76.11.1.2.1.1)**,
  - **Postecom CA2 (OID 2.5.29.32.0),**
  - **Postecom CA3 (OID 2.5.29.32.0)**,
- a partire dal 01/07/2016 fino al 31/03/2017:
  - **Postecom CA5 (OID 1.3.76.11.1.1.6.1)**.

I certificati si riferiscono a chiavi crittografiche presenti a bordo di carte SIM per servizi di telefonia mobile, utilizzate nell'ambito di servizi aggiunti offerti dall'operatore mobile

3.5 Certificati di sicurezza (firma codice)

OID	Descrizione
1.3.76.11.1.1.6.2	Certificati di sicurezza (Firma codice)

I certificati di sicurezza per firma codice sono stati rilasciati dalla seguente Autorità di certificazione:

- **Postecom CS1 (OID 1.3.76.11.1.1.6.1)**

Questa tipologia di certificati permette di firmare codici per scopi diversi (eseguibili, ActiveX, plugin, applet ecc.), in modo da garantire l'identità del soggetto firmatario (che può essere o una persona fisica o una persona giuridica) e assicurare l'integrità del codice.

3.6 Certificati SSL e firma codice

OID	Tipo di supporto
1.3.76.11.1.1.4.1	Certificati SSL Web server
1.3.76.11.1.1.4.2	Certificati SSL Client
1.3.76.11.1.1.4.3	Certificati Firma codice

I certificati SSL e firma codice sono stati rilasciati dalle seguenti Autorità di certificazione:

- **Postecom CS2 (OID 1.3.76.11.1.1.3.1)**,
- **Postecom CS3 (OID 1.3.76.11.1.1.3.1)**.

a partire dal 01/07/2016 i certificati SSL e firma codice sono stati rilasciati anche dall'Autorità di certificazione:

- **Postecom CA4 (OID 1.3.76.11.1.1.6.1).**

I Certificati SSL per Web Server permettono di instaurare una comunicazione protetta tra un web server ed un browser. In particolare, garantiscono l'identità del sito al quale ci si collega, l'identità della Società titolare del sito e assicurano la cifratura delle informazioni scambiate.

I certificati per firma codice sono utilizzati per garantire l'identità del soggetto firmatario (che può essere o una persona fisica o una persona giuridica) e assicurare l'integrità del codice.

3.7 Certificati per CNS

OID	Tipologia di certificati
1.3.76.11.1.3.1	Certificato di autenticazione per CNS

Postecom ha emesso certificati di autenticazione per carte CNS per conto di Province e Regioni Autonome, tramite Autorità di certificazione appositamente dedicate, nell'ambito della fornitura, da parte di Sogei verso i cittadini, di carte CNS con funzioni di Tessera Sanitaria.